DETAILED ACTION

Claims 1-22 are currently presented and have been examined.

Response to Arguments

The Examiner notes for the record that a replacement specification has been filed in this case and the citations provided by the Examiner in reference to prior art that was admitted by the Applicant and used in the rejection of the claims refer to the pages of the response that was provided by the Applicant on 24 March 2009 and as such have been incorrect. For example, the Examiner has been referring to pages 4-5 when the Examiner should have been referring to pages 3-4.

The Applicant argues that "No alleged APPA discloses, teaches, or suggests providing integrity protection of messages, when the claim terms are given their 'broadest reasonable interpretation consistent with the specification'" The Applicant provides wherein the specification defines "integrity protection" on page 5 lines 12-14 as "comprises any method of assuring that information sent from an originating source is not accidentally or maliciously altered or destroyed during communication from the source to the receiver". As shown previously by the Examiner, the Applicant admitted that the "IEEE 802.11 standard offers secure communications services such as authentication and encryption via a wired equivalence privacy mechanism". Such "encryption" is known to be used to assure that information sent from an originating source is not altered or destroyed during communication as encryption protocols produce the exact same data when decrypted. Furthermore, the standard as provided by the Applicant disclosed wherein each data frame sent from a source to a receiver

contains "a frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC)" (see section 7.1 of the "IEEE 802.11" standard) wherein "The WEP ICV is 32 bits. The WEP Integrity Check algorithm is CRC-32, as defined in [section] 7.1.3.6" (see section 8.2.3) and "correct decipherment shall be verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received MPDU is in error and an error indication is sent to MAC management. MSDUs with erroneous MPDUs...shall not be passed to LLC". (see section 8.2.3) Therefore, the Applicant clearly admitted to such "integrity protection".

The Applicant also argues the Examiner's interpretation of an "access control list" as recited in claim 9. However, the claim only nominally recites "providing" such data which, given that the claim is drawn to a method, could be done by any element and it is also the view of the Examiner that "providing" any sort of data without any further recitation of how the data is processed or otherwise transformed does not further limit the scope of the claim and, therefore, the Examiner has interpreted the claim in its broadest reasonable interpretation and maintains the interpretation as given previously. See MPEP 2111.04.

Therefore, the claims are not in condition for allowance.

Claim Rejections

Claims 1-4, 6, 8-18, 20, and 22 are rejected in view of the Applicant's admitted Prior Art ("AAPA"). The Applicant described subject matter in the specification at page 3, lines 12-17, page 6, lines 23-29, page 21, lines 13-27, page 22, line 23-page 23, line

2, page 25, lines 5-14, page 25, line 23-page 26, line 2, and page 27, lines 4-12 that was by another, therefore, this statement is construed by the Examiner that this statement constitutes an admission of prior art and any subject matter associated with these statements are construed to be prior art applicable to the claims. See MPEP 2129 and *Riverwood Int'l Corp. v. R.A. Jones & Co.*, 324 F.3d 1346, 1354, 66 USPQ2d 1331, 1337 (Fed Cir. 2003).

Regarding claim 1, "AAPA" disclosed a method of providing to a client communications device by a server communications device, access to a network, the server communications device comprising a subscription module for facilitating authentication of a subscriber to the network ("module that is physically inseparable from the server communications device"; see page 9, lines 20-22), the method comprising the steps of:

establishing a communications link between the client communications device and the server communications device; and between the server communications device and the client communications device via the communications link; receiving a message by the server communications device from the client communications device via the communications link, the message being addressed to the subscription module; performing, by a processing means of the server communications device outside the subscription module, the following steps:

providing integrity protection of the received message to determine whether the received message is authentic (using "keys"); determining whether the received message is authorized to address the subscription module; and forwarding (upon a

"successful" connection) the received message to the subscription module, if the processing means of the server communications device has determined the received message as being authentic and if the processing means of the server communications device has determined the received message as being authorized to address the subscription module; otherwise rejecting the received message ("unsuccessful"). (see at least pages 4-5 of the specification, specifically the "802.11" admitted prior art, the specification of which was filed in the 18 July 2005 IDS, specifically section 8.1)

Regarding claim 2, "AAPA" disclosed the method according to claim 1, wherein the step of providing integrity protection further comprises calculating, based on a secret session key, a respective message authentication code for each of the communicated messages; and including the calculated message authentication code into the corresponding communicated message. (see at least page 22, line 23-page 23, line 2)

Regarding claim 3, "AAPA" disclosed the method according to claim 2, wherein the step of establishing a communications link between the client and server communications devices comprises determining a secret session key based on a shared secret between the server and client communications devices. (see at least page 25, line 23-page 26, line 2)

Regarding claim 4, "AAPA" disclosed the method according to claim 3, wherein the method further comprises providing the shared secret by performing a secure pairing procedure including receiving a passcode by at least one of the client communications device and the server communications device. (see at least page 27, lines 4-12)

Regarding claim 6, "AAPA" disclosed the method according to claim 3, wherein the communications link has a secret link key related to it and the method further comprises providing the shared secret by calculating the shared secret using the secret link key as an input. (see at least page 25, lines 5-14)

Regarding claim 8, "AAPA" disclosed the method according to claim 1, wherein the method further comprises determining, for the messages communicated from the client communications device to the server communications device, whether the message is authorised to address the subscription module. (see at least page 3, lines 12-17 and page 7, lines 1-6 of the specification)

Regarding claim 9, "AAPA" disclosed the method according to claim 8, wherein the method further comprises: providing a shared secret between the client communications device and the server communications device; and providing an access control list stored in the server communications device in relation to at least one of the shared secret and the client communications device. (see at least page 27, lines 4-12) (note that the server specifically interacts with the client using cryptography, therefore, a strong association between the server and the client is established and the cryptographic settings used between the client and the server on the server is considered to encompass the claimed "access control list" where the server is in a generic and nominal relation to the "client communications device", therefore allowing the client access to the server based on the agreed upon cryptographic settings)

Regarding claim 15, "AAPA" disclosed the method according to claim 14, wherein the access control list is stored in a protected database. (note that

cryptographic settings are essential to the security of the connection and are stored in confidence at the server and are thus considered to be "protected")

Claims 10-12 are also rejected since these claims recite substantially the same limitations as recited in claim 1.

Claims 13 and 22 are also rejected since these claims recite substantially the same limitations as recited in claims 1 and 8 in combination.

Claim 14 is rejected since this claim recites substantially the same limitations as recited in claim 9.

Claims 16-20 are also rejected since these claims recite substantially the same limitations as recited in claims 2-6 respectively.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claim 5 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over "AAPA".

Regarding claim 5, "AAPA" disclosed the method according to claim 4.

"AAPA" did not expressly disclose wherein the passcode is at the most 48 bits long.

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to create a passcode which is at most 48 bits long, since it has been held that discovering an optimum value of a result effective variable involves only routine skill in the art. In re Boesch, 617 F.2d 272, 205 USPQ 215 (CCPA 1980).

Claim 19 is also rejected since this claim recites substantially the same limitations as recited in claim 5.

Claims 7 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "AAPA" in view of US Patent 6,449,473 to Raivisto.

Regarding claim 7, "AAPA" disclosed the method according to any one of claims 2 through 6.

"AAPA" did not expressly disclose wherein the method further comprises: incorporating a value of a first counter in each of the messages communicated from the client communications device to the server communications device, the first counter being indicative of the number of messages communicated from the client communications device to the server communications device; and incorporating a value of a second counter in each of the messages communicated from the server communications device to the client communications device, the second counter being

indicative of the number of messages communicated from the server communications device to the client communications device; and wherein the step of calculating a respective message authentication code for each of the communicated messages comprises calculating a message authentication code for each of the communicated messages and the corresponding counter value, however, Raivisto did disclose these limitations (the counter value being a "sequence number"; see at least column 3, line 66-column 4, line 26)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of these references since Raivisto disclosed that using counter values in the calculation of the message authentication code allows for the specific advantage of recalculating the code for stronger security and to enable synchronous recalculation between the client and the server (see at least column 4, line 5-9). Therefore, based on this specific motivation and that the references are analogous to one another in the context of message security and communication security, one of ordinary skill would have been motivated to modify the teachings of "AAPA" to include the subject matter taught in Raivisto in order to arrive at a more robust and secure communication link between a client and a server.

Claim 21 is also rejected since this claim recites substantially the same limitations as recited in claim 7.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to George C. Neurauter, Jr. whose telephone number is (571)272-3918. The examiner can normally be reached on the hours between 8:30am-5:00pm Eastern.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia Dollinger, can be reached on 571-272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/George C Neurauter, Jr./
Primary Examiner, Art Unit 2443